



PROGETTO SETTIMANALE

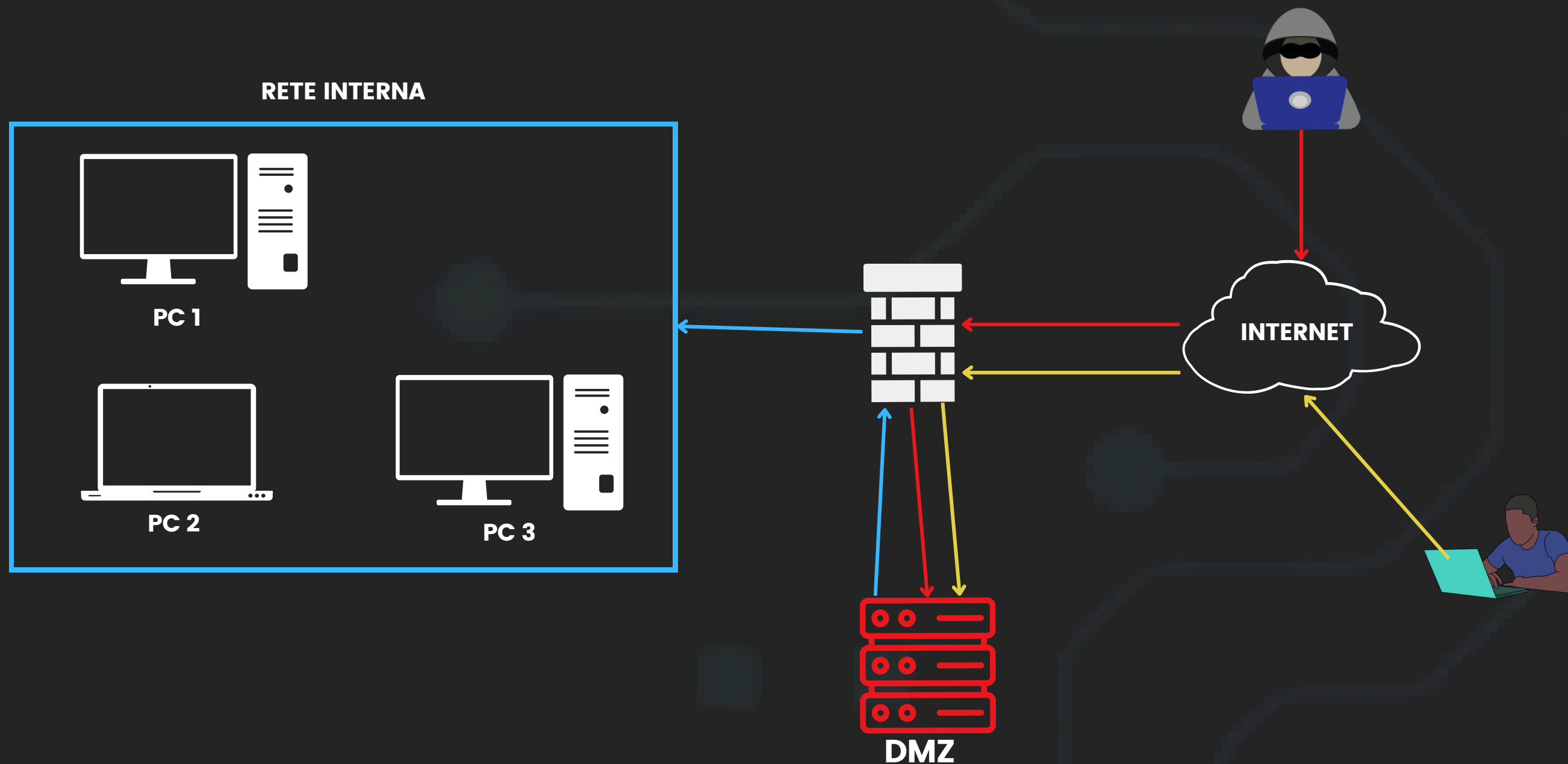
EPICODE

Giovanni Pisapia

SCENARIO INZIALE

Nell' esercizio di oggi ci veniva chiesto:

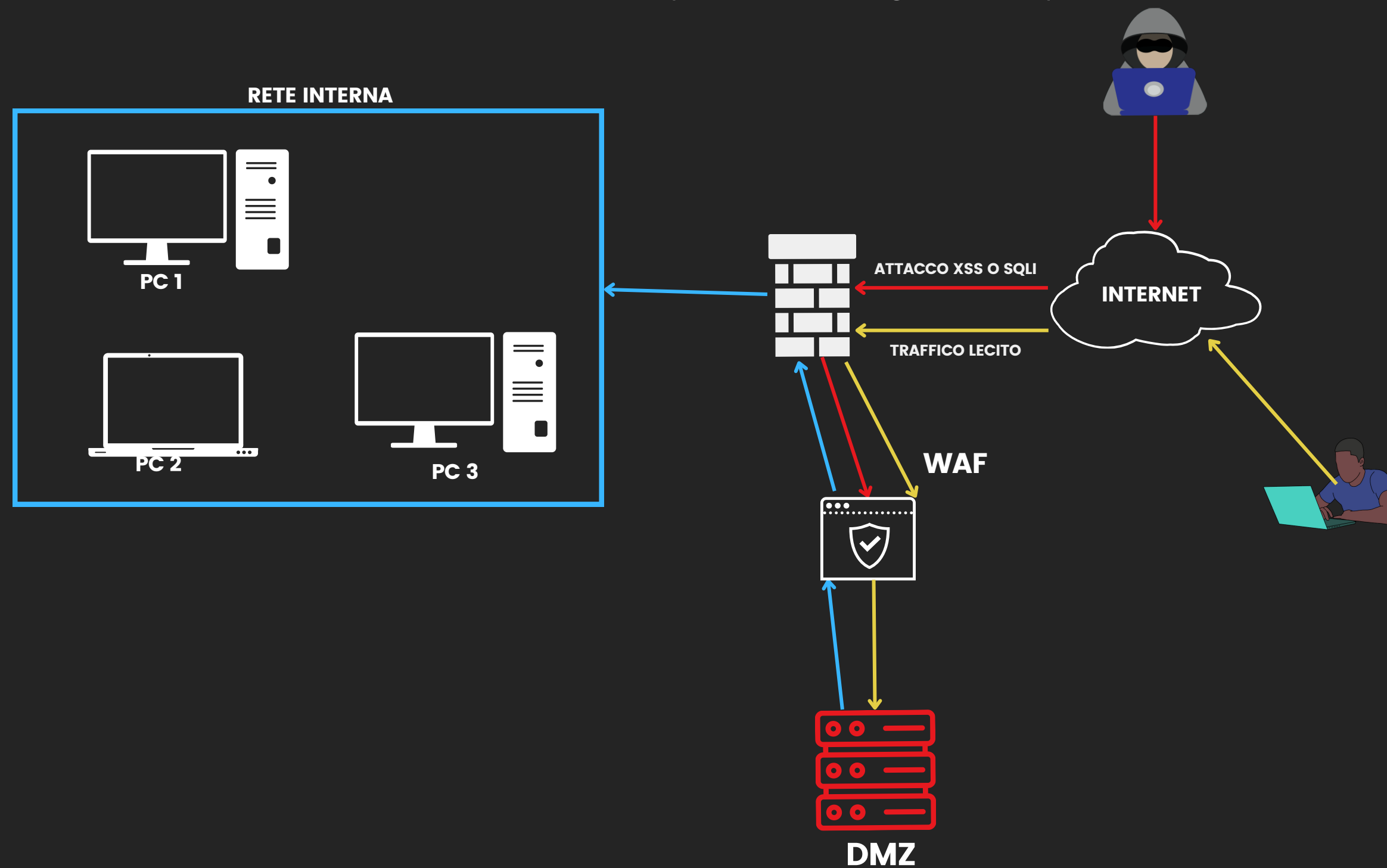
- Effettuare zioni preventive per evitare un attacco xss e sqli
- Analizzare un attacco tramite link
- Risposta ad un incidente causato da un malware
- Di creare una soluzione completa
- Modificare l'infrastruttura di rete integrando altri elenti di sicirezza



1. AZIONI PREVENTIVE

Per evitare attacchi di tipo xss e sqli:

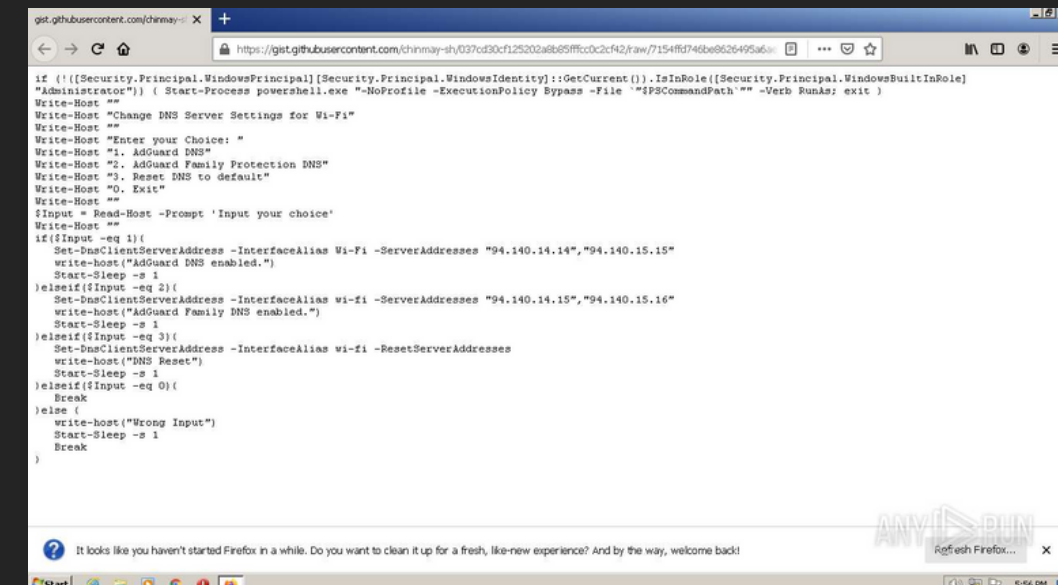
- Inserimento di un WAF (Web Application Firewall) nell'infrastruttura di rete. Il WAF può aiutare a rilevare e bloccare attacchi di tipo SQLi, XSS e altre vulnerabilità comuni delle applicazioni web. Il WAF viene utilizzato per monitorare e filtrare il traffico HTTP/HTTPS verso l'applicazione e-commerce.
- Validare e sanificare attentamente tutti i dati di input forniti dagli utenti prima di utilizzarli nell'applicazione.



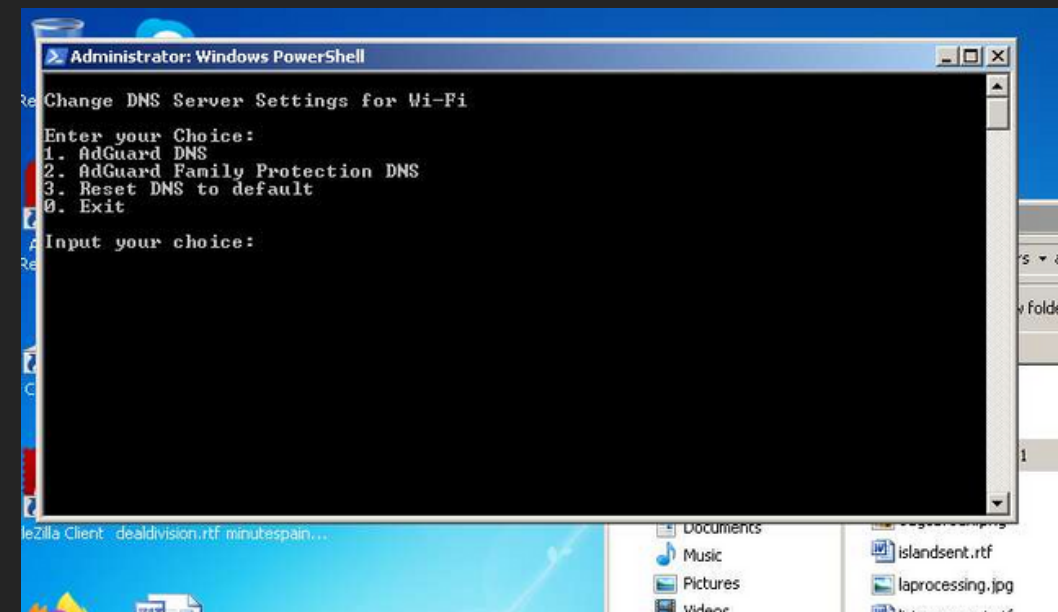
1. ANALISI ATTACCO

Analisi link 1:

- Quando ricevo un link sospetto da un utente, la prima cosa che faccio è domandargli se lo ha aperto. In caso affermativo, gli consiglio di cambiare immediatamente le sue credenziali per garantire la sicurezza del suo account. Successivamente, seguo queste azioni per analizzare il link in modo sicuro:
- Prima di tutto, effettuo una ricerca online per cercare informazioni sul link. In questo caso, si può notare che si tratta di uno short link creato con TinyURL, che permette di nascondere il link reale. Questo aspetto può risultare sospetto.
- Dopo aver effettuato la ricerca, copio il link senza aprirlo direttamente dal mio browser. In questo modo, posso evitare di espormi a eventuali minacce potenziali.
- Successivamente, mi sposto in un ambiente protetto come una sandbox o utilizzo un servizio di analisi dinamica come Any.Run. Questi strumenti creano un ambiente virtualizzato che mi consente di aprire il link in modo sicuro senza rischi per il mio sistema.
- Una volta all'interno dell'ambiente protetto, osservo attentamente il comportamento del link. Monitoro le richieste di rete che vengono effettuate, l'esecuzione di eventuali script e l'apertura di file. Queste informazioni mi aiutano a determinare se il link è dannoso o meno.
- In siti il link malevolo porta ad un link https://gist.githubusercontent.com/chinmay-sh/037cd30cf125202a8b85ffcc0c2cf42/raw/7154ffd746be8626495a6ae7073889972c458ddf/DNS_Changer.ps1 che scarica un script in powershell che permette di modificare le impostazioni DNS del computer, indirizzando il traffico verso server controllati dall'attaccante.



```
if ([Security.Principal.WindowsPrincipal]::GetCurrent().IsInRole([Security.Principal.WindowsBuiltInRole] "Administrator")) { Start-Process powershell.exe -NoProfile -ExecutionPolicy Bypass -File "$PSCommandPath" -Verb RunAs; exit }
Write-Host ""
Write-Host "Change DNS Server Settings for Wi-Fi"
Write-Host ""
Write-Host "Enter your Choice: "
Write-Host "1. AdGuard DNS"
Write-Host "2. AdGuard Family Protection DNS"
Write-Host "3. Reset DNS to default"
Write-Host "0. Exit"
Write-Host ""
$Input = Read-Host -Prompt 'Input your choice'
Write-Host ""
if ($Input -eq 1) {
    Set-DnsClientServerAddress -InterfaceAlias Wi-Fi -ServerAddresses "94.140.14.14","94.140.15.15"
    Write-Host("AdGuard DNS enabled.")
    Start-Sleep -s 1
}
elseif ($Input -eq 2) {
    Set-DnsClientServerAddress -InterfaceAlias Wi-Fi -ServerAddresses "94.140.14.15","94.140.15.16"
    Write-Host("AdGuard Family DNS enabled.")
    Start-Sleep -s 1
}
elseif ($Input -eq 3) {
    Set-DnsClientServerAddress -InterfaceAlias Wi-Fi -ResetServerAddresses
    Write-Host("DNS Reset")
    Start-Sleep -s 1
}
elseif ($Input -eq 0) {
    Break
}
else {
    Write-Host("Wrong Input")
    Start-Sleep -s 1
    Break
}
```



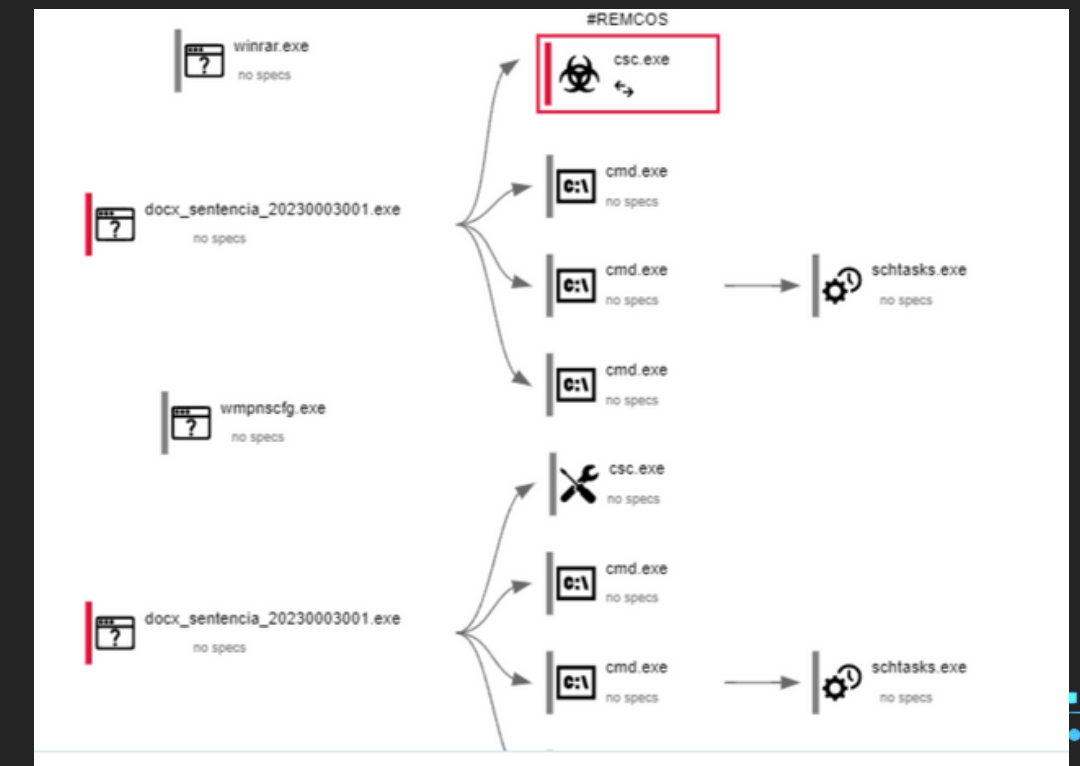
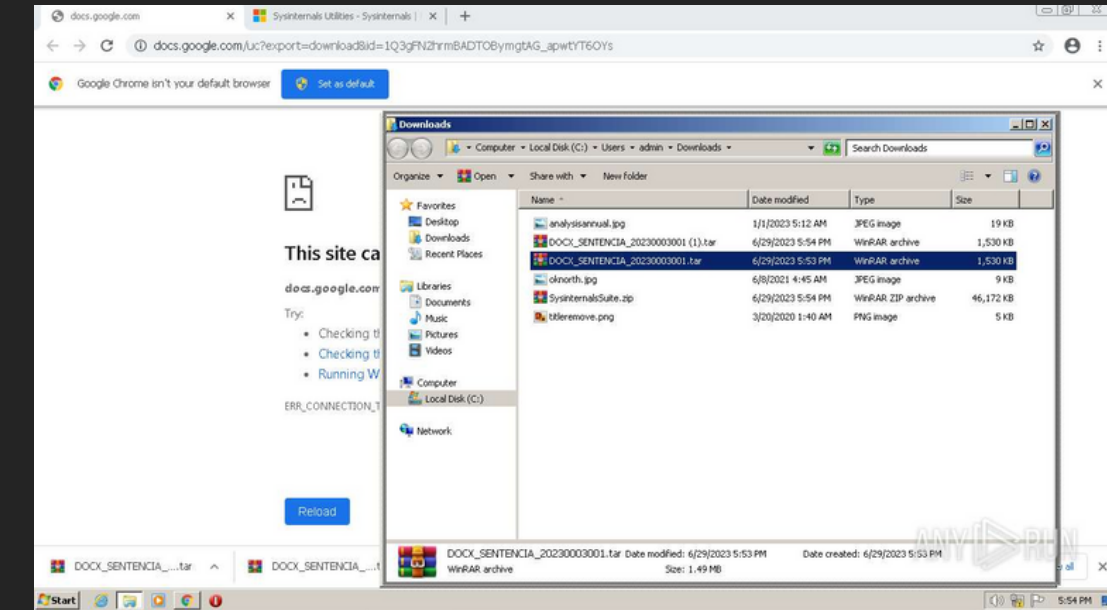
1. ANALISI ATTACCO 2

Analisi link 2:

Quando ricevo un link sospetto da un utente, la prima cosa che faccio è domandargli se lo ha aperto. In caso affermativo, gli consiglio di cambiare immediatamente le sue credenziali per garantire la sicurezza del suo account. Successivamente, seguo queste azioni per analizzare il link in modo sicuro:

- Effettuo una ricerca online per cercare informazioni sul link. In questo caso, si può notare che si tratta di uno short link creato con TinyURL, che permette di nascondere il link reale. Questo aspetto può risultare sospetto.
- Copio il link senza aprirlo direttamente dal mio browser. In questo modo, posso evitare di espormi a eventuali minacce potenziali.
- Mi sposto in un ambiente protetto, come una sandbox o utilizzo un servizio di analisi dinamica come Any.Run. Questi strumenti creano un ambiente virtualizzato che mi consente di aprire il link in modo sicuro senza rischi per il mio sistema.
- Una volta all'interno dell'ambiente protetto, osservo attentamente il comportamento del link. Monitoro le richieste di rete che vengono effettuate, l'esecuzione di eventuali script e l'apertura di file. Queste informazioni mi aiutano a determinare se il link è dannoso o meno.

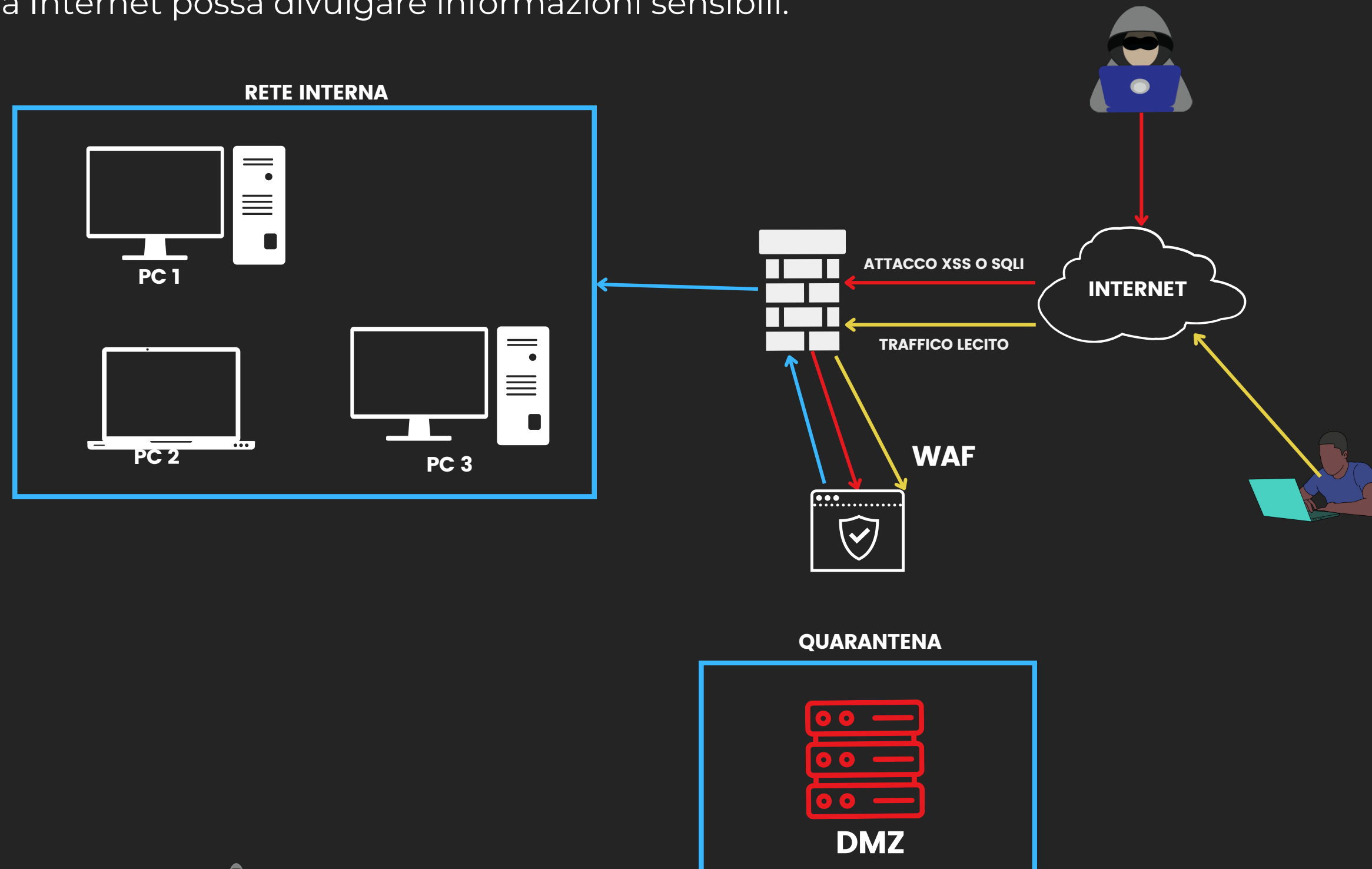
Dopo aver analizzato il link, ho scoperto che il file scaricato sembra essere un file PDF legittimo, ma in realtà è un file eseguibile in formato .exe che contiene il malware Remcos. Remcos è un tipo di malware RAT (Remote Access Trojan) che compromette la sicurezza del sistema e agisce come una backdoor, eseguendo comandi dannosi e persistenti. Il suo obiettivo principale è la violazione della privacy dell'utente, rubando credenziali, registrando le tastiere premute e acquisendo informazioni personali dell'utente.



3. RESPONSE

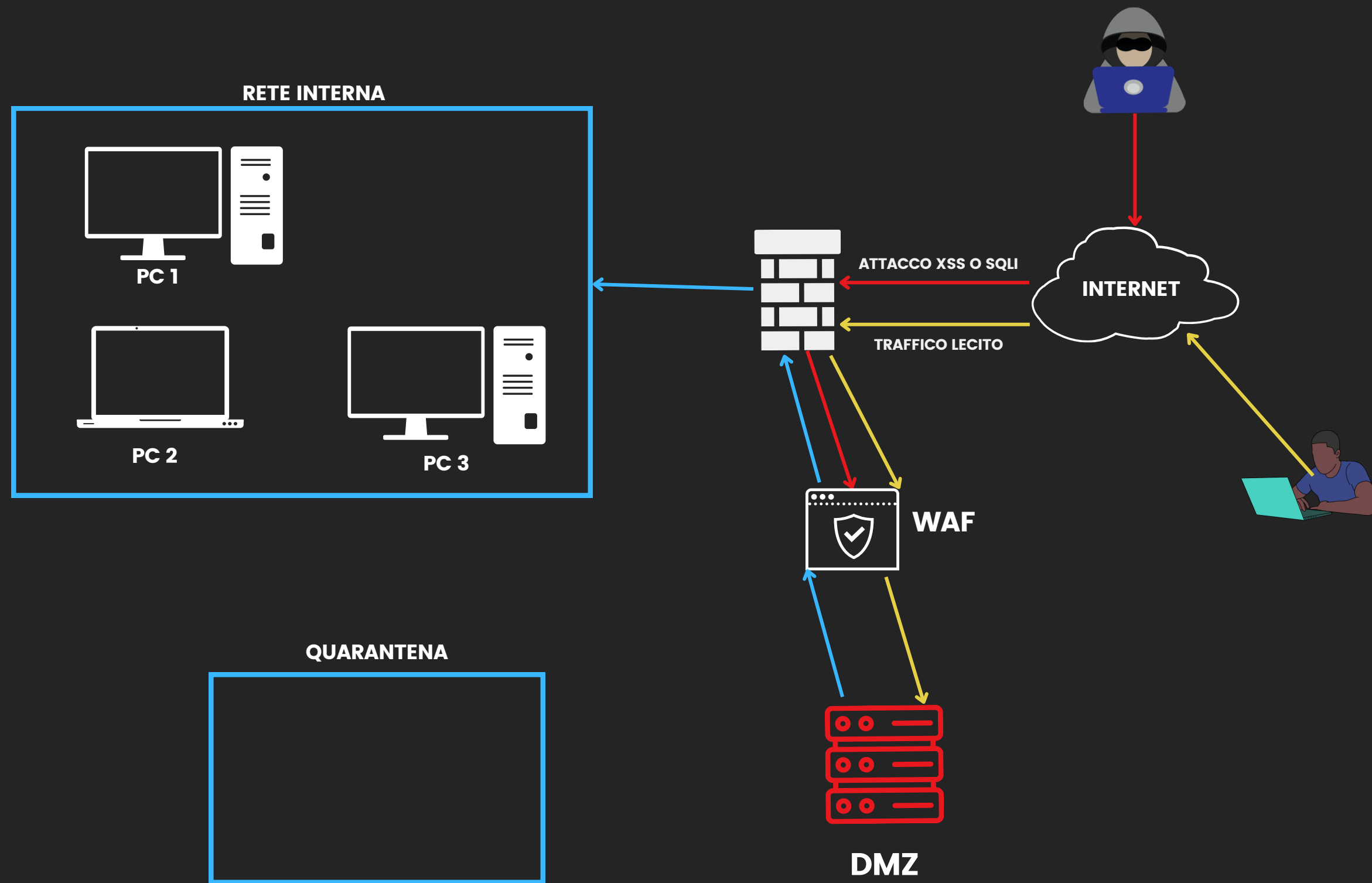
Se un'applicazione web viene infettata da un malware:

- Dopo aver isolato il sistema compromesso, dovremmo procedere alla sua rimozione dalla rete o allo spegnimento, a seconda della gravità dell'attacco. Se l'attacco è in corso e il sistema non può essere prontamente ripristinato, potrebbe essere necessario rimuovere fisicamente il dispositivo per garantire la sicurezza degli altri sistemi nella rete. L'isolamento del sistema comporta il rischio che la macchina ancora collegata a Internet possa divulgare informazioni sensibili.

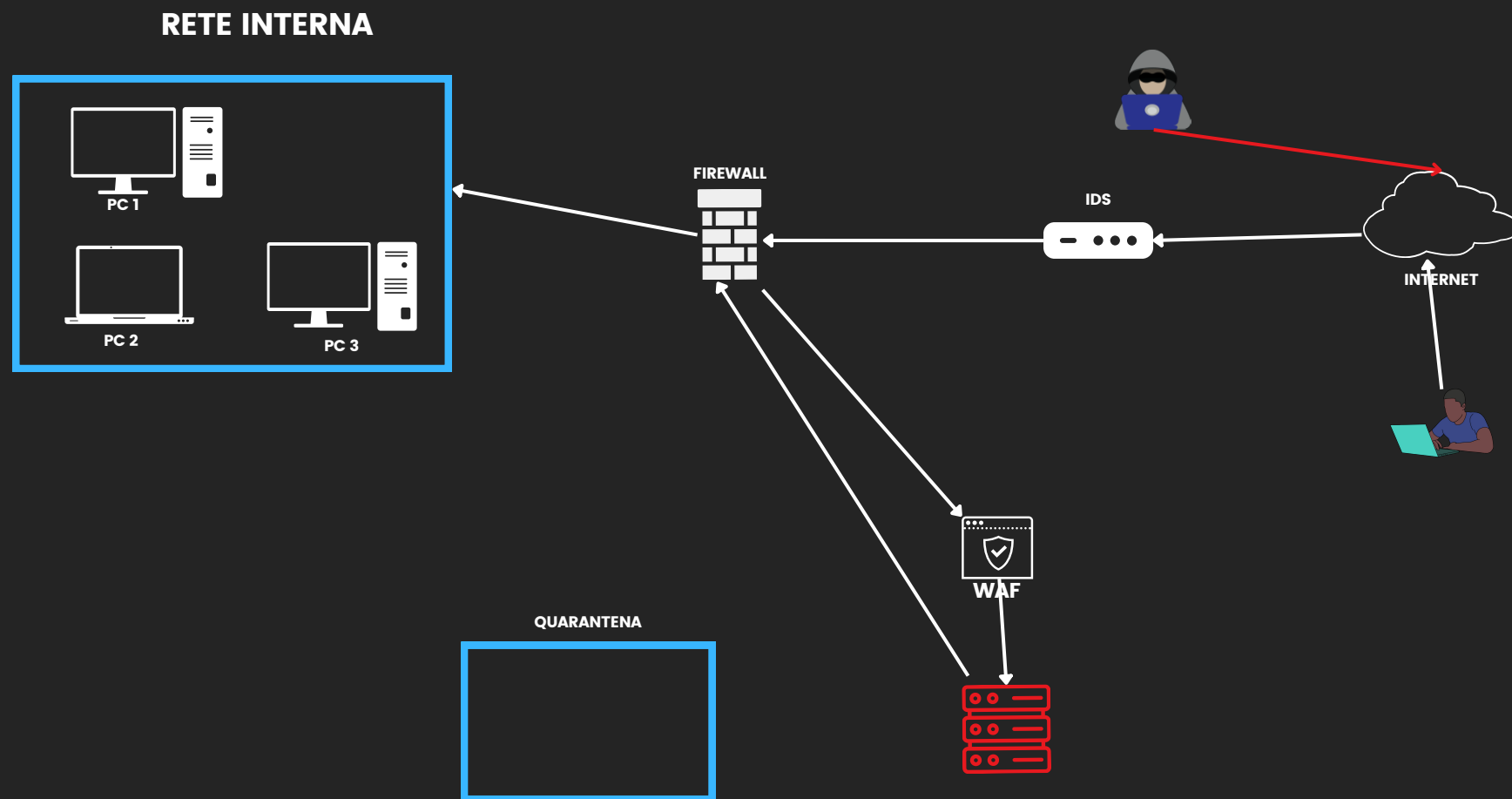


4.SOLUZIONE COMPLETA

La soluzione completa viene attuata mediante l'implementazione di una rete di isolamento in caso di incidenti.



5. MODIFICA AGGRESSIVA DELL'INFRASTRUTTURA



Per una modifica più aggressiva della struttura di rete possiamo:

- Integrare una segmentazione di rete come vlan o lan
- Un IDS (Intrusion Detection System) è un sistema progettato per rilevare e rispondere agli attacchi informatici. Funziona monitorando il traffico di rete o gli eventi di sistema alla ricerca di comportamenti sospetti o anomalie.
- Avere più UPS (Uninterruptible Power Supply) è un dispositivo elettronico progettato per fornire energia elettrica di emergenza a un sistema o a un'apparecchiatura quando la fonte di alimentazione principale viene interrotta o si verifica un'interruzione di corrente
- NAS per fare backup della web application
- Virtual site: Un virtual site è un ambiente di riserva che viene creato utilizzando la virtualizzazione. Consente di replicare e ripristinare le risorse critiche su infrastrutture virtuali in caso di incidenti, riducendo i costi e accelerando il ripristino.
- Avere una rete isolata così in caso di incidenti si può isolare un sistema.
- SIEM (Security Information and Event Management) è una soluzione software che offre la gestione centralizzata degli eventi di sicurezza e delle informazioni di sicurezza, permettendo di raccogliere, analizzare e correlare i dati provenienti da diverse fonti. Fornisce monitoraggio in tempo reale, rilevamento delle minacce e risposta agli incidenti, consentendo una migliore sicurezza informatica.